UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/089,478	03/28/2002	Yoichiro Sako	7246/64967	1150

7590 03/06/2006

EXAMINER
SHAW, YIN CHEN

Jay H Maioli
Cooper & Dunham
1185 Avenue of the Americas
New York, NY 10036

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/089,478	SAKO ET AL.	
	Examiner	Art Unit	
	Yin-Chen Shaw	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,9,23-29,32,34-42 and 46-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,9,23-29,32,34-42 and 46-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This written action is responding to the amendment dated 12/16/2005.
2. Claims 7-8, 10-22, 30, 31, 33, 43-45 are cancelled. Claims 1-6, 9, 23-29, 32, 34-42, 46, and 48 are amended.
3. Claims 1-6, 9, 23-29, 32, 34-42, and 46-48 have been submitted for examination.
4. Claims 1-6, 9, 23-29, 32, 34-42, and 46-48 have been examined and rejected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-2, 9, 32, 36-38, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Imamura et al. (U.S. Patent 6,453,369) and further in view of Kurihara (U.S. Patent 6,069,956).

   a. *Referring to Claim 1:*

      As per Claim 1, Imamura et al. discloses a recording and reproducing method for a record medium, the method comprising the steps of: performing one of a recording process and a reproducing process for the record medium **[access to the memory medium data reading and/or writing (line 7-8, Abstract). In the embodiment of the present**

invention, a magneto-optical disk (MO) is employed as a memory medium (hereinafter referred to as a medium) for recording data (lines 14-16, Col. 4)].

reading record medium information from the record medium when data are recorded to the record medium and reproduced from the record medium on which the record medium information has been recorded **[When a magneto-optical disk in which the device identifier is recorded is inserted into a specific storage device, data reading/writing control is provided in accordance with the relationship between the device identifier of the storage device and the device identifier recorded in the medium (lines 14-18, Col. 5). The writing in a medium of the device identifier is performed by the magneto-optical disk controller (ODC) 11 (lines 24-25, Col. 5). At step S103, data in the medium information management area on the medium are read, and at step S104, the security information (device identifier) recorded in the security area are read (lines 62-65, Col. 5)]**;

reading apparatus information from a recording and reproducing apparatus for the record medium **[A device identifier inherent to a magneto-optical disk device (hereinafter referred to as a storage device) (lines 9-11, Col. 5). Compared with the device identifier of the storage device 1 in which the medium is currently loaded (lines**

9-10, Col. 6); *this means the device identifier information is first read from the magnet-optical device*];

comparing the record medium information from the record medium with the apparatus information read from the apparatus **[at step S106, the device identifier recorded on the medium is compared with the device identifier of the storage device 1 in which the medium is currently loaded in order to determine whether the two device identifies match (lines 7-11, Col. 6)]**.

Imamura et al. further disclose the perform one of recording process and reproducing process for the record medium **[reads data from and/or writes data to a memory medium (lines 51-52, Col. 1)]**, and when the record medium information read from the record medium matches the apparatus information read from the apparatus **[the device identifier recorded on the medium is compared with the device identifier of the storage device 1 in which the medium is currently loaded in order to determine whether the two device identifiers match. When the two device identifiers match, the process then advances to step S108 (lines 8-13, Col. 6)]**. Imamura et al. disclose the security information, such as a device identifier, address information, password, or other suitable information, may be compared between the record medium and the apparatus **[whereat the device identifier included in the security area is compared with the device identifier of the**

storage device into which the medium has been loaded (lines 37-40, Col. 11 and Fig. 5). In the above described embodiments of the present invention, the security information (a device identifier, an address information, a password, etc.) to be recorded in the security area may be encoded to enhance the secrecy (lines 52-55, Col. 11)], Imamura et al. do not expressly disclose (1) the information is the encryption key version information (2) using an encryption key corresponding to the apparatus encryption key version information stored in the apparatus, and (3) the steps of encrypting and decrypting processes. However, Kurihara discloses (1) the key version number information associated with the scramble key **[A first embodiment of the present invention is directed to detection of switching or changeover of scramble keys on the basis of information concerning a version number (lines 47-49, Col. 4). The version number represents the values imparted to the scramble keys in the updating or renewing sequence thereof (lines 66-67, Col. 4, line 1, Col. 5, and Fig. 16)]**, (2) using the scrambling key corresponding to the key version information in the apparatus **[In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view**

for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16); ***where the key managing table unit is within the device***], and (3) the step of encrypting and decrypting **[the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). A descrambling function that a correct descramble key is retrieved from descramble key information available (lines 51-52, Col. 16)]**.

Imamura et al. and Kurihara are analogous art because they are from similar technology relating to relating to the digital data information security and data accessing. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Imamura et al. with Kurihara. The modification would be obvious since one of ordinary skill in the art would be motivated to provide a communication apparatus and a communication method in which

changeover or change of the scramble key is detected on the basis of a version number and thereby scramble the application data by using a scramble key which corresponds to the detected scramble key information (lines 42-44 and 46-48, Col. 2 from Kurihara). Therefore, it would have been obvious to combine Imamura et al. with Kurihara to obtain the invention as specified in claim 1.

b. *Referring to Claims 2 and 38:*

As per Claim 2, Imamura et al. and Kurihara disclose the recording and reproducing method for the record medium as set forth in claim 1. In addition, Imamura et al. disclose the method further comprising the step of:

determining which of the record medium information read from the record medium and the apparatus information read from the apparatus is information that corresponds to a later generation when the record medium type information read from the record medium does not match the apparatus type information read from the apparatus **[the device identifier recorded on the medium is compared with the device identifier of the storage device 1 in which the medium is currently loaded in order to determine whether the two device identifiers match. When the two device identifiers match, the process then advances to step S108 (lines 8-13, Col. 6). When at step S06, the two device identifiers do not match (lines 16-17, Col. 6); *this means***

that when two identifiers do not match, one of them must be larger (or later) than the other] and Kurihara discloses the information is the version information and corresponds to the scrambling key **[In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16)]**.

As per Claim 38, the rejection of Claim 37 is incorporated. In addition, Claim 38 encompasses limitations that are similar to those of Claim 2. Therefore, it is rejected with the same rationale applied against Claim 2 above.

c. *Referring to Claim 9:*

As per Claim 9, Imamura et al. and Kurihara disclose the recording and reproducing method as set forth in claim 1. In addition, Kurihara discloses wherein the encryption key corresponding to the apparatus encryption key version is stored in the apparatus **[In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16); *where the key managing table unit, provides the scrambling key corresponds to the version number, is within the device*]**.

d. *Referring to Claim 32:*

As per Claim 32, Imamura et al. disclose a record medium on which address information including information that corresponding to a generation of information **[a magneto-optical disk (MO) is employed**

as a memory medium (hereinafter referred to as a medium) for recording data (lines 14-15, Col. 4). At step 802, the address information in the security area are read (lines 32-33, Col. 11). At step S907, the device identifier included in the security identifier included in the security information. Security information in the security area is a device identifier inherent to a magneto-optical disk device (hereinafter referred to as a storage device), such as a serial number]. Imamura et al. do not expressly disclose the encryption key version information and an encryption key for performing an encrypting process for data to be recorded is recorded. However, Kurihara discloses the key version information and its correspondence to the generation of the scrambling key, which is used for encrypting the data **[In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key,**

the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16)]. Imamura et al. and Kurihara are analogous art because they are from similar technology relating to relating to the digital data information security and data accessing. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Imamura et al. with Kurihara. The modification would be obvious since one of ordinary skill in the art would be motivated to provide a communication apparatus and a communication method in which changeover or change of the scramble key is detected on the basis of a version number and thereby scramble the application data by using a scramble key which corresponds to the detected scramble key information (lines 42-44 and 46-48, Col. 2 from Kurihara). Therefore, it would have been obvious to combine Imamura et al. with Kurihara to obtain the invention as specified in claim 32.

e. *Referring to Claim 36:*

As per Claim 36, Imamura et al. disclose a recording and reproducing method for a record medium, the method comprising the steps of:

reading record medium information from the record medium when data are one of recorded to the record medium and reproduced from the record medium on which the record medium information is recorded **[When a magneto-optical disk in which the device identifier is**

recorded is inserted into a specific storage device, data reading/writing control is provided in accordance with the relationship between the device identifier of the storage device and the device identifier recorded in the medium (lines 14-18, Col. 5). The writing in a medium of the device identifier is performed by the magneto-optical disk controller (ODC) 11 (lines 24-25, Col. 5). At step S103, data in the medium information management area on the medium are read, and at step S104, the security information (device identifier) recorded in the security area are read (lines 62-65, Col. 5)];

reading apparatus information of key information from a recording and reproducing apparatus for the record medium **[A device identifier inherent to a magneto-optical disk device (hereinafter referred to as a storage device) (lines 9-11, Col. 5). Compared with the device identifier of the storage device 1 in which the medium is currently loaded (lines 9-10, Col. 6); *this means the device identifier information is first read from the magnet-optical device*]**;

comparing the record medium information read from the record medium with the apparatus information read from the apparatus **[at step S106, the device identifier recorded on the medium is compared with the device identifier of the storage device 1 in which the medium is**

currently loaded in order to determine whether the two device identifies match (lines 7-11, Col. 6)]; and

controlling one of a recording and a reproducing operation corresponding to a compared result of the comparing step **[data reading/writing control is provided in accordance with the relationship between the device identifier of the storage device and the device identifier recorded in the medium (lines 14-18, Col. 5)]**.

Imamura et al. do not expressly disclose the encryption key version information corresponding to the encryption key. However, Kurihara discloses the key version information and its correspondence to the generation of the scrambling key, which is used for encrypting the data **[In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble**

key (lines 51-53, Col. 8 and Fig. 1 and 16)]. Imamura et al. and Kurihara are analogous art because they are from similar technology relating to relating to the digital data information security and data accessing. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Imamura et al. with Kurihara. The modification would be obvious since one of ordinary skill in the art would be motivated to provide a communication apparatus and a communication method in which changeover or change of the scramble key is detected on the basis of a version number and thereby scramble the application data by using a scramble key which corresponds to the detected scramble key information (lines 42-44 and 46-48, Col. 2 from Kurihara). Therefore, it would have been obvious to combine Imamura et al. with Kurihara to obtain the invention as specified in claim 36.

f. *Referring to Claim 37:*

As per Claim 37, Imamura et al. and Kurihara disclose the recording and reproducing method for the record medium as set forth in claim 36. In addition, Imamura et al. disclose the step of:

recording data to the record medium and reproducing data from the record medium using information corresponding to the apparatus type information stored in the apparatus when the record medium type information read from the record medium matches the apparatus type

information read from the apparatus **[the device identifier recorded on the medium is compared with the device identifier of the storage device 1 in which the medium is currently loaded in order to determine whether the two device identifiers match. When the two device identifiers match, the process then advances to step S108, whereat the security is released and the reading of data from the medium and the writing of data to it are permitted (lines 8-15, Col. 6)]**, and Kurihara discloses the step of encrypting and decrypting **[the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). A descrambling function that a correct descramble key is retrieved from descramble key information available (lines 51-52, Col. 16)]** and the information is the version information and corresponds to the scrambling key **[In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15**

manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16)].

g. *Referring to Claim 46:*

As per Claim 46, Imamura et al. and Kurihara disclose the recording and reproducing method as set forth in claim 36. Kurihara further discloses the encryption key **[scramble key (line 48, Col. 4)]** in additional to Imamura et al. disclose recorded in address information recorded in the record medium **[address information to be used to control writing of data are stored in a predetermined area on the memory medium (lines 9-11, Col. 2). At step S802, the address information in the security area are read (lines 32-33, Col. 11). The security information (device identifier) recorded in the security area are read (lines 64-65, Col. 5)]**.

6. Claims 3-6 and 39-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Imamura et al. (U.S. Patent. 6,453,369) and Kurihara (U.S. Patent 6,069,956) and further in view of Ito (U.S. Patent 6,496,978).

a. *Referring to Claims 3 and 39:*

As per Claim 3, Imamura et al. and Kurihara disclose the recording and reproducing method for the record medium as set forth in claim 2. Imamura et al. disclose canceling the recording process and the reproducing process **[the reading/writing of data is inhibited (lines 17-18, Col. 6)]**, and Kurihara discloses the key version information and its correspondence to the generation of the scrambling key **[In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16)]** and the step of encrypting and decrypting **[the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). A descrambling function that a correct**

descramble key is retrieved from descramble key information available (lines 51-52, Col. 16)] in additional to a result of the determining step as in Claim 2. Imamura et al. and Kurihara do not expressly disclose the record medium information read from the record medium is information that corresponds to a generation later than a generation represented by the apparatus information read from the apparatus. However, Ito disclose the comparison of the version number is performed to determine if the one associated with the EPROM (recording medium such as CD-ROM) is more recent than the one associated with the ROM in the system **[When the EPROM 5 is an EPROM conforming to the microcomputer control system, version information (version number a) stored in the storage area 201 of the ROM 2 is compared with version information (version number b) stored in the storage area 211 of the EPROM 5 (step 33), and if the comparison show that the version number b of the EPROM 5 is more recent (lines 3-9, Col. 4). In this embodiment, as an information recording medium, there can be used pressed CD-ROM disks, DVD-ROM disks, write-once CD-R disks, DVD-R disks, erasable CD-RW disks, and DVD-RAM disks, and the use of these media would make additional operations on version changes simpler than the use of an EPROM (lines 41-46, Col. 10)]**. Imamura et al., Kurihara, and Ito are analogous art because they are from similar

technology relating to relating to the digital data information security and data accessing. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Imamura et al. and Kurihara with the further comparison result disclosed by Ito to effectively control the information access. The modification would be obvious since one of ordinary skill in the art would be motivated to have a microcomputer control system which is controlled on the basis of program or data stored in memory (lines 8-9, Col. 1 from Ito). Therefore, it would have been obvious to combine Imamura et al. and Kurihara with Ito to obtain the invention as specified in claim 3.

As per Claim 39, the rejection of Claim 38 is incorporated. In addition, Claim 39 encompasses limitations that are similar to those of Claim 3. Therefore, it is rejected with the same rationale applied against Claim 3 above.

b. *Referring to Claims 4 and 40:*

As per Claim 4, Imamura et al., Kurihara, and Ito disclose the recording and reproducing method for the record medium as set forth in claim 3. In addition, Imamura et al. disclose a display for displaying data **[a display 4 on which data are displayed (line 51, Col. 4)]**, and Kurihara discloses indication for prompting a user to obtain encryption key version information and a corresponding encryption key that corresponds to the

later generation of encryption key **[Communication apparatus and a communication method in which changeover or change of the scramble key is detected on the basis of a version number (indicating a sequence in which the scramble key is changed for updating thereof) and an information indicator (indicating whether ECM data for transmission is valid or not) (lines 46-52, Col. 2). The individual data resulting from the demulitplexing may be reproduced by an output device such as a display (lines 33-35, Col. 16). In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16)]**.

As per Claim 40, the rejection of Claim 39 is incorporated. In addition, Claim 40 encompasses limitations that are similar to those of Claim 4. Therefore, it is rejected with the same rationale applied against Claim 4 above.

c. *Referring to Claims 5 and 41:*

As per Claim 5, Imamura et al. and Kurihara disclose the recording and reproducing method for the record medium as set forth in claim 2. Imamura et al. disclose performing the recording process and reproducing process **[the reading of data from the medium and the writing of data to it are permitted (lines 14-15, Col. 6)]**, and Kurihara discloses the key version information and its correspondence to the generation of the scrambling key **[In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying**

information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16)] and the step of encrypting and decrypting **[the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). A descrambling function that a correct descramble key is retrieved from descramble key information available (lines 51-52, Col. 16)]** in addition to a result of the determining step as in Claim 2. Imamura et al. and Kurihara do not expressly disclose the apparatus information read from the apparatus is information that represents a generation later than a generation corresponding to the record medium information read from the record medium. However, Ito disclose the comparison of the version number is performed to determine if the one associated with the ROM in the system is more recent than the one associated with the EPROM (recording medium such as CD-ROM) **[When the EPROM 5 is an EPROM conforming to the microcomputer control system, version information (version number a) stored in the storage area 201 of the ROM 2 is compared with version information (version number b) stored in the storage area 211 of the EPROM 5 (step 33), and if the comparison show that the version number b of the EPROM 5 is more recent, control is transferred to step 35; if the version number a of the ROM 2 is more recent (lines 3-10, Col. 4). In this**

embodiment, as an information recording medium, there can be used pressed CD-ROM disks, DVD-ROM disks, write-once CD-R disks, DVD-R disks, erasable CD-RW disks, and DVD-RAM disks, and the use of these media would make additional operations on version changes simpler than the use of an EPROM (lines 41-46, Col. 10)]. Imamura et al., Kurihara, and Ito are analogous art because they are from similar technology relating to relating to the digital data information security and data accessing. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Imamura et al. and Kurihara with the further comparison result disclosed by Ito to effectively control the information access. The modification would be obvious since one of ordinary skill in the art would be motivated to have a microcomputer control system which is controlled on the basis of program or data stored in memory (lines 8-9, Col. 1 from Ito). Therefore, it would have been obvious to combine Imamura et al. and Kurihara with Ito to obtain the invention as specified in claim 5.

As per Claim 41, the rejection of Claim 38 is incorporated. In addition, Claim 41 encompasses limitations that are similar to those of Claim 5. Therefore, it is rejected with the same rationale applied against Claim 5 above.

d. *Referring to Claims 6 and 42:*

As per Claim 6, Imamura et al., Kurihara, and Ito disclose the recording and reproducing method for the record medium as set forth in claim 5. In addition, Imamura et al. further disclose a display for displaying data **[a display 4 on which data are displayed (line 51, Col. 4)]** and Kurihara discloses indication that represents that the record encryption key version information read from the record medium is former encryption key version information **[Communication apparatus and a communication method in which changeover or change of the scramble key is detected on the basis of a version number (indicating a sequence in which the scramble key is changed for updating thereof) and an information indicator (indicating whether ECM data for transmission is valid or not) (lines 46-52, Col. 2). The individual data resulting from the demulitplexing may be reproduced by an output device such as a display (lines 33-35, Col. 16). In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-**

division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16)].

As per Claim 42, the rejection of Claim 41 is incorporated. In addition, Claim 42 encompasses limitations that are similar to those of Claim 6. Therefore, it is rejected with the same rationale applied against Claim 6 above.

7. Claims 34-35, and 47-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Imamura et al. (U.S. Patent. 6,453,369) and Kurihara (U.S. Patent 6,069,956) and further in view of Osakabe (U.S. Patent 6,894,961).

   a. *Referring to Claims 34 and 47:*

      As per Claim 34, Imamura et al. Kurihara disclose the record medium as set forth in claim 32. In addition In addition, Imamura et al. disclose the address information as in Claim 32. Imamura et al. and Kurihara do not expressly disclose information is recorded in a lead-in area of the disc-shaped record medium. However, Osakabe discloses the optical disk has information such as the disk type (disk information), maker (manufacturing) and speed information recorded in the lead-in area as ATIP information **[ATIP information that is recorded in pre-grooves**

located in a lead-in area of an optical disk (lines 3-4, Abstract). Optical disk 12 has the information indicative of the disk type and maker as well as the disk-applicable-recording-speed information recorded within the lead-in (lines 26-29, Col. 9); *where the optical disk with pre-grooves is a disc-shaped record medium*]. Imamura et al., Kurihara, and Osakabe are analogous art because they are from similar technology relating to the digital data information processing and accessing, such as CD-ROM processing technique. It would have been obvious to one of ordinary skill in the art at the time of invention was made to have address information taught in Imamura et al. be stored at the lead-in area of the disk disclosed in Osakabe. The modification would be obvious since one of ordinary skill in the art would be motivated to realize the ATIP information recorded in the lead-in area of the optical disk may contain special (lines 31-34, Col. 5 from Osakabe). Therefore, it would have been obvious to combine Imamura et al. and Kurihara with Osakabe to obtain the invention as specified in claim 34.

As per Claim 47, the rejection of Claim 46 is incorporated. In addition, Claim 47 encompasses limitations that are similar to those of Claim 34. Therefore, it is rejected with the same rationale applied against Claim 34 above.

b. *Referring to Claim 35 and 48:*

As per Claim 35, Imamura et al., Kurihara, and Osakabe disclose the record medium as set forth in claim 34. Imamura et al. disclose the information is embedded at predetermined intervals in the address information **[At step S802, the address information in the security area are read, and at step 803 a check is performed to determine whether there are security information in the security area (lines 32-34, Col. 11). At step S103, data in the medium information management area on the medium are read, and at step S104, the security information (device identifier) recorded in the security area are read (lines 62-65, Col. 5). Read address information to be used to control reading of data and/or write address information to be used to control writing of data are stored in a predetermined area on the memory medium (lines 8-11, Col. 2)]**. Imanura et al. further disclose the address information as in Claim 11 in addition to Kurihara discloses the encryption key version information **[The version number represents the values imparted to the scramble keys (lines 66-67, Col. 4 and Fig. 16)]** and Osakabe discloses recorded such that grooves pre-formed on the disc-shaped record medium are wobbled **[recorded in the pre-groove wobbles or pre-pits of the optical disk (lines 31-33, Col. 2)]**.

As per Claim 48, the rejection of Claim 47 is incorporated. In addition, Claim 48 encompasses some limitations that are similar to those of Claim 35. Therefore, it is rejected with the same rationale applied against Claim 35 above.

8. Claims 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Imamura et al. (U.S. Patent 6,453,369) and further in view of Osakabe (U.S. Patent 6,894,961) and Kurihara (U.S. Patent 6,069,956).

a. *Referring to Claim 23:*

As per Claim 23, Imamura et al. disclose a recording and reproducing apparatus for a record medium, the apparatus comprising:

a head portion for scanning the record medium on which record medium type information is recorded **[head sensor 100, a data reading/writing diode 101, and a detector 102 for detecting the inclination of a head (lines 39-41, Col. 4)]**;

a storing portion for storing storing information **[The device identifier of the storage device is stored in the flash ROM provided for the magneto-optical disk controller (ODC) (lines 50-52, Col. 5)]**; and

a controlling portion for reading the record medium information from the record medium **[a control unit which includes a magneto-optical disk controller (ODC) which employs firmware to implement a method according to the present invention (line 29-32, Col. 4). The**

magneto-optical disk controller (ODC) 11, which is provided with flash ROM for the storage of firmware, has an analysis function for analyzing SCSI commands received from the computer 2, and a coordination function for interacting with the MPU 12, in response to a SCSI command, to provide data writing/reading control of the mechanism controller 10 (lines 52-58, Col. 4). At step S103, data in the medium information management area on the medium are read, and at step S104, the security information (device identifier) recorded in the security area are read (lines 62-65, Col. 5)];

reading the storing information from the storing portion **[A device identifier inherent to a magneto-optical disk device (hereinafter referred to as a storage device) (lines 9-11, Col. 5). Compared with the device identifier of the storage device 1 in which the medium is currently loaded (lines 9-10, Col. 6); *this means the device identifier (storing type) information is first read from the magnet-optical device*]**;

comparing the record medium information read from the record medium with the storing information read from the storing portion **[the device identifier recorded on the medium is compared with the device identifier of the storage device 1 in which the medium is currently loaded in order to determine whether the two device identifiers match (lines 8-11, Col. 6)]**; and

causing the processing portion to perform one of a recording process and a reproducing process for the record medium using information responding to the storing information stored in the storing portion when the record medium information read from the record medium matches the storing information read from the storing portion when the data are recorded to the record medium and reproduced from the record medium **[When the two device identifiers match, the process then advances to step S108, whereat the security is released and the reading of data from the medium and the writing of data to it are permitted (lines 12-15, Col. 6)]**.

Imamura et al. do not expressly disclose the remaining limitations of the claim. However, Osakabe discloses:

a signal processing portion for supplying record data to be recorded on the record medium to the head portion and for performing a decoding process for data read from the record medium by the head portion **[an EFM encoder 33 for encoding into the EFM format (lines 28-30, Col. 8), and the thus-encoded data is delivered, via the control circuit 20 and an ALPC (Auto Laser Power Control) circuit 35, to the optical head 16, which in turn, records the data onto the optical disk 12 (lines 30-34, Col. 8). EFM (Eight to Fourteen Modulation) decoder 21 EFM-decodes each disk readout signal that is output from the**

optical head 16 as the head 16 reads the optical disk 12 (lines 64-66, Col. 7)].

In addition, Kurihara discloses (1) the key version information and a scrambling key corresponding to the key version information **[The version number represents the values imparted to the scramble keys (lines 66-67, Col. 4). In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16)]** and (2) an encryption and a decryption process **[the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). A**

descrambling function that a correct descramble key is retrieved from descramble key information available (lines 51-52, Col. 16)]. Imamura et al., Osakabe, and Kurihara are analogous art because they are from similar technology relating to the digital data information processing and accessing, such as CD-ROM processing technique. It would have been obvious to one of ordinary skill in the art at the time of invention was made to have signal processing components to handle the information processing during the data read/writing process and scramble key related to the device identifier, such as the key version information. The modification would be obvious since one of ordinary skill in the art would be motivated to have (1) recording on the optical disk with minimized errors (lines 37-38, Col. 1 from Osakabe), and (2) a communication apparatus and a communication method in which changeover or change of the scramble key is detected on the basis of a version number and thereby scramble the application data by using a scramble key which corresponds to the detected scramble key information (lines 42-44 and 46-48, Col. 2 from Kurihara). Therefore, it would have been obvious to combine Imamura et al. with Osakabe and Kurihara to obtain the invention as specified in claim 23.

b. *Referring to Claim 24:*

As per Claim 24, Imamura et al., Osakabe, and Kurihara disclose the recording and reproducing apparatus for the record medium as set forth

in claim 23. In addition, Imamura et al. disclose wherein said controlling portion includes: a comparing portion for comparing the record medium information read from the record medium with the storing information read from the storing portion **[The magneto-optical disk controller (ODC) 11, which is provided with flash ROM for the storage of firmware, has an analysis function for analyzing SCSI commands received from the computer 2, and a coordination function for interacting with the MPU 12, in response to a SCSI command, to provide data writing/reading control of the mechanism controller 10 (lines 52-58, Col. 4). Data reading/writing control is provided in accordance with the relationship between the device identifier of the storage device and the device identifier recorded in the medium. For example, only when the two identifiers match, the reading/writing of data is permitted (lines 16-20, Col. 5)]**, and Kurihara discloses the encryption key version information **[The version number represents the values imparted to the scramble keys (lines 66-67, Col. 4 and Fig. 16)]**.

c. *Referring to Claim 25:*

As per Claim 25, Imamura et al., Osakabe, and Kurihara disclose the recording and reproducing apparatus for the record medium as set forth in claim 23. In addition, Imamura et al. disclose wherein said controlling portion determines which of the record medium information read from

the record medium and the storing information read from the storing portion is information that corresponds to a later generation when the record medium information read from the record medium does not match the storing information read from the storing portion **[The magneto-optical disk controller (ODC) 11, which is provided with flash ROM for the storage of firmware, has an analysis function for analyzing SCSI commands received from the computer 2, and a coordination function for interacting with the MPU 12, in response to a SCSI command, to provide data writing/reading control of the mechanism controller 10 (lines 52-58, Col. 4). Data reading/writing control is provided in accordance with the relationship between the device identifier of the storage device and the device identifier recorded in the medium (lines 15-17, Col. 5). The device identifier recorded on the medium is compared with the device identifier of the storage device 1 in which the medium is currently loaded in order to determine whether the two device identifiers match. When the two device identifiers match, the process then advances to step S108 (lines 8-13, Col. 6). When at step S06, the two device identifiers do not match (lines 16-17); *this means that when two identifiers do not match, one of them must be larger (or later) than the other*]**, and Kurihara discloses the key version information and its correspondence to the generation of the scrambling key, which is used

for encrypting the data **[In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16)]**.

9. Claims 26-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Imamura et al. (U.S. Patent 6,453,369), Osakabe (U.S. Patent 6,894,961) and Kurihara (U.S. Patent 6,069,956) and further in view of Ito (U.S. Patent 6,496,978).

   a. *Referring to Claim 26:*

      As per Claim 26, Imamura et al., Osakabe, and Kurihara disclose the recording and reproducing apparatus for the record medium as set forth in claim 25, wherein the controlling portion causes the signal processing portion to cancel the process **[the reading/writing of data is inhibited**

(lines 17-18, Col. 6 from Imamura)], and Kurihara discloses the key version information and its correspondence to the generation of the scrambling key, which is used for encrypting the data **[In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16)]**. Imamura et al., Osakabe, and Kurihara do not expressly disclose the record medium type information read from the record medium is type information that corresponds to a generation later than a generation corresponding to the storing information read from said storing portion. However, Ito discloses the comparison of the version number is performed to determine if the one associated with the EPROM (recording medium such as CD-ROM) is more recent than the one associated with the ROM in the system **[When the EPROM 5 is an**

EPROM conforming to the microcomputer control system, version information (version number a) stored in the storage area 201 of the ROM 2 is compared with version information (version number b) stored in the storage area 211 of the EPROM 5 (step 33), and if the comparison show that the version number b of the EPROM 5 is more recent (lines 3-9, Col. 4). In this embodiment, as an information recording medium, there can be used pressed CD-ROM disks, DVD-ROM disks, write-once CD-R disks, DVD-R disks, erasable CD-RW disks, and DVD-RAM disks, and the use of these media would make additional operations on version changes simpler than the use of an EPROM (lines 41-46, Col. 10)]. Imamura et al., Osakabe, Kurihara, and Ito are analogous art because they are from similar technology relating to the digital data information processing and accessing, such as CD-ROM processing and control technique. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Imamura et al., Osakabe, and Kurihara with the further comparison result disclosed by Ito to effectively control the information access. The modification would be obvious since one of ordinary skill in the art would be motivated to have a microcomputer control system which is controlled on the basis of program or data stored in memory (lines 8-9, Col. 1 from Ito). Therefore, it would have been

obvious to combine Imamura et al., Osakabe, and Kurihara with Ito to obtain the invention as specified in claim 26.

b. *Referring to Claim 27:*

As per Claim 27, Imamura et al., Osakabe, Kurihara, and Ito disclose the recording and reproducing apparatus for the record medium as set forth in claim 26, the apparatus further comprising:

disclose a displaying portion; wherein said controlling portion causes the displaying portion **[display 4 (line 51, Col. 4 from Imamura et al.), which is linked to the ODC 11 (Fig. 1 from Imamura)]** to perform an indication for prompting a user to obtain the encryption key version information and a corresponding encryption key that corresponds the later generation of encryption key **[Communication apparatus and a communication method in which changeover or change of the scramble key is detected on the basis of a version number (indicating a sequence in which the scramble key is changed for updating thereof) and an information indicator (indicating whether ECM data for transmission is valid or not) (lines 46-52, Col. 2 from Kurihara). The individual data resulting from the demulitplexing may be reproduced by an output device such as a display (lines 33-35, Col. 16). In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble**

key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5 from Kuraihara). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16 from Kurihara)].

c. *Referring to Claim 28:*

As per Claim 28, Imamura et al., Osakabe, and Kurihara disclose the recording and reproducing apparatus for the record medium as set forth in claim 25, wherein the controlling portion causes signal processing portion to perform the process using information corresponding to the storing information stored in the storing portion as in claim 23. In addition, Kurihara discloses the key version information and its correspondence to the generation of the scrambling key, which is used for encrypting the data **[In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5). FIG. 16 is a view for illustrating**

imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16)]. Imamura et al., Osakabe, and Kurihara et al. do not expressly disclose when the storing information read from the storing portion is information that corresponds to a generation later than a generation corresponding to the record medium information read from the record medium. However, Ito discloses the comparison of the version number is performed to determine if the one associated with the ROM in the system is more recent than the one associated with the EPROM (recording medium such as CD-ROM) **[When the EPROM 5 is an EPROM conforming to the microcomputer control system, version information (version number a) stored in the storage area 201 of the ROM 2 is compared with version information (version number b) stored in the storage area 211 of the EPROM 5 (step 33), and if the comparison show that the version number b of the EPROM 5 is more recent, control is transferred to step 35; if the version number a of the ROM 2 is more recent (lines 3-10, Col. 4). In this embodiment, as an information**

recording medium, there can be used pressed CD-ROM disks, DVD-ROM disks, write-once CD-R disks, DVD-R disks, erasable CD-RW disks, and DVD-RAM disks, and the use of these media would make additional operations on version changes simpler than the use of an EPROM (lines 41-46, Col. 10)]. Imamura et al., Osakabe, Kurihara, and Ito are analogous art because they are from similar technology relating to the digital data information processing and accessing, such as CD-ROM processing and control technique. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Imamura et al., Osakabe, and Kurihara with the further comparison result disclosed by Ito to effectively control the information access. The modification would be obvious since one of ordinary skill in the art would be motivated to have a microcomputer control system which is controlled on the basis of program or data stored in memory (lines 8-9, Col. 1 from Ito). Therefore, it would have been obvious to combine Imamura et al., Osakabe, and Kurihara with Ito to obtain the invention as specified in claim 28.

d. *Referring to Claim 29:*

As per Claim 29, Imamura et al., Osakabe, Kurihara, and Ito disclose the recording and reproducing apparatus for the record medium as set forth in claim 28, the apparatus further comprising:

a displaying portion, wherein the controlling portion causes said displaying portion **[display 4 (line 51, Col. 4 from Imamura et al.), which is linked to the ODC 11 (Fig. 1)]** to perform an indication that represents that the record medium encryption key version information read from the record medium is former type information **[Communication apparatus and a communication method in which changeover or change of the scramble key is detected on the basis of a version number (indicating a sequence in which the scramble key is changed for updating thereof) and an information indicator (indicating whether ECM data for transmission is valid or not) (lines 46-52, Col. 2 from Kurihara). The individual data resulting from the demulitplexing may be reproduced by an output device such as a display (lines 33-35, Col. 16). In the application data encryption processing circuit 1, the time-division frames for the application data concerned are scrambled by using the scramble key received from the scramble key managing table 15 via the time-division frame controller 13 (lines 47-51, Col. 5 from Kuraihara). FIG. 16 is a view for illustrating imagearily in what manner the scramble key information is stored in the scramble key managing table 15. Referring to the figure, the scramble key managing table 15 manages for each of the time-division frame ID of the ECM data the time-division frame ID, for the application data to be subject to the**

scrambling, the scramble key, the version number and the attributed identifying information of the scramble key (lines 51-53, Col. 8 and Fig. 1 and 16 from Kurihara)].

Response to Arguments

10. Applicant's remark filed on Dec. 16, 2005 has been fully considered.

    a. Applicant's amended claims filed on Dec. 16, 2005 have been fully considered. The prior art by Kurihara (U.S. Patent 6,069,956) has been found and used, in combination, with other previously cited references. See the rejection above.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office Action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

    A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be

calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

a. Green et al. (U.S. Patent 5,081,677) disclose the crypto facility compares the version number of the current master key to that of the request and, in the event of an unequal condition, generates an exception. A Version Number is supplied and stored in a version number register 100, associated with the current master key. As part of the execution of a normal crypto operation, the reference master key version number 109 is passed, along with the source operands 118, to the crypto facility. The RMKVN is also compared with the master key version number register 110. The comparison is done in the master key version number comparison circuit 117. The RMKVN is compared with zero. This comparison is done in the zero-test circuit 119. Normal crypto operations are rejected if the RMKVN is zero or if it does not match the MKVN Register.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 8:15 to 4:15 M-F. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Yen Vu can be reached on 571-272-3859. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YCS

Feb. 28, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100